日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　２月１９日

出願番号
Application Number: 特願２００３－０４０６９２

[ST. 10/C]: [ＪＰ２００３－０４０６９２]

出願人
Applicant(s): 千代田メインテナンス株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２００４年　３月　３日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００４－３０１６２８３

【書類名】　特許願
【整理番号】　0030004-02
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/60
　　G06F 19/00
【発明者】
　【住所又は居所】　茨城県鹿島郡旭村箕輪１６３２番地　千代田メインテナンス株式会社内
　【氏名】　井上　義章
【発明者】
　【住所又は居所】　茨城県鹿島郡旭村箕輪１６３２番地　千代田メインテナンス株式会社内
　【氏名】　吉川　祐一
【特許出願人】
　【識別番号】　391051360
　【氏名又は名称】　千代田メインテナンス株式会社
【代理人】
　【識別番号】　100081927
　【弁理士】
　【氏名又は名称】　北條　和由
【手数料の表示】
　【予納台帳番号】　010917
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9723892
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　偽造品の市場流通を防止する製品認証システム

【特許請求の範囲】

【請求項１】　インターネットを介して製品の認証を行うシステムで、

認証対象の製品に認証素子として埋め込まれる非接触タグで、製品認証システムの管理者しか知り得ない固有のＩＤを持ち、ＩＤを電子データとして本体に記録させた非接触タグと、

非接触タグのＩＤデータを読み取るリーダで、製品認証システムの管理者しか知り得ない固有のＩＤを持ち、ＩＤを電子データとして本体に記録させ、インターネットに接続して通信する手段を持つリーダと、

非接触タグのＩＤおよび付帯情報のデータ、非接触タグが埋め込まれた製品情報のデータ、リーダのＩＤおよび付帯情報のデータを格納するデータベースで、インターネットに接続して通信する手段を持つデータベースと、

データベースに格納されたデータの読み出しやデータベースへのデータの書き込みを行うデータサーバで、インターネットに接続して通信する手段を持つデータサーバと、

インターネットに接続されたリーダから送信されたリーダのＩＤデータおよび非接触タグのＩＤデータをデータベースに格納されたデータと照合して、リーダおよび非接触タグの認証を行う認証サーバで、インターネットに接続して通信する手段を持つ認証サーバと、で構成される製品認証システムで、

製品認証システムの利用者に非接触タグおよびリーダを配布する前に、データサーバが非接触タグおよびリーダのＩＤデータを読み込み、データファイルを作成してデータベースに格納する手段と、

製品認証システムの利用者に非接触タグおよびリーダが配布された後に、インターネットに接続されたリーダが自分自身のＩＤデータを認証サーバに送信し、認証サーバが受信したリーダのＩＤデータをデータベースに格納されたリーダのデータファイルと照合する手段と、

認証サーバが、同一のＩＤデータとの照合がなされたリーダに対してリーダが認証された旨を通知し、製品に埋め込まれた非接触タグのＩＤデータの送信を促

す手段と、

認証されたリーダが、製品に埋め込まれた非接触タグのＩＤデータを読み込んで認証サーバに送信し、認証サーバが受信した非接触タグのＩＤデータをデータベースに格納された非接触タグのデータファイルと照合する手段と、

認証サーバが、同一のＩＤデータとの照合がなされた非接触タグが認証された旨を、非接触タグのＩＤデータを送信したリーダに対して通知する手段と、

を備えた製品認証システム。

【請求項２】　アプリケーションサービスプロバイダ（ＡＳＰ）事業者が管理および運営し、インターネットを介した製品認証サービスをＡＳＰ方式で提供することを特徴とする、請求項１に記載の製品認証システム。

【請求項３】　リーダの利用者に対して、リーダの管理者および利用者しか知り得ない固有のパスワードを割り当てることにより、利用者側に２重のＩＤを持させる製品認証システムで、

データサーバが、割り当てられたパスワードのデータを読み込み、配布されたリーダのＩＤデータと対応づけた付帯情報としてデータファイルを作成し、データベースに格納する手段と、

認証サーバが、リーダの認証通知後に利用者のパスワード入力を要求し、利用者の端末から入力され送信されたパスワードのデータを受信し、データベースに格納されたデータファイルと照合する手段と、

認証サーバが、同一のパスワードデータとの照合がなされたパスワードが認証された旨を、パスワードデータを送信した利用者端末に対して通知する手段と、

を備えた請求項１または２に記載の製品認証システム。

【請求項４】　製品認証システムの利用者である製品のメーカに配布されたリーダおよび利用者端末が、製品の名称、型式、製造年月日、製造場所などの製品情報データを非接触タグのIDデータと対応づけてデータサーバに送信する手段と、

データサーバが製品情報データを受信して、埋め込まれた非接触タグのＩＤデータと対応づけた付帯情報としてデータファイルを作成し、データベースに格納する手段と、

を備えた請求項１～３の何れかに記載の製品認証システム。

【請求項５】　非接触タグの製造メーカが、非接触タグのＩＤと非接触タグの供給先である製品のメーカを対応づけたデータファイルを作成して、データサーバに送信する手段と、

データサーバが、データファイルを受信してデータベースに格納する手段と、

認証サーバが、リーダから送信された非接触タグのＩＤデータを受信して、データベースに格納された非接触タグのデータファイルでＩＤと供給先の対応を照合する手段と、

を備えた請求項１～４の何れかに記載の製品認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、市場に出回る偽造品が流通経路に侵入するのを防ぐことにより、流通経路を形成するメーカ、販売業者、流通業者、消費者の利益を保護するため、流通段階における製品認証サービスをＡＳＰ方式で提供する製品認証システムに関するものである。

【０００２】

【従来の技術】

消費者が腕時計、バッグ、衣類などの装身具を購入するとき、それがどこのメーカの製品であるかというブランドは商品選びの重要な決め手となる。消費者が装身具に求める価値は、単に必要な機能を満たしているだけでなく、自己表現の手段として優れていることである。ブランドは自己のこだわりを端的に表現しうるという点で、商品にとって大きな付加価値である。よって、有力なブランドを持つメーカは、自社製品であることが一目でわかるように、製品に独自の統一されたデザインを施したり、登録商標やロゴマークなどをわざわざ見える位置に表示したりする。消費者はそのような製品を携行するだけで、周囲にメーカのブランドを誇示して自己のこだわりを表現することができる。このような消費志向にあって、メーカはシェア拡大を図るために、ブランド力を高めて自社商品の付加価値をより大きくすることに力を注いできた。

【０００３】

ところが一方においてこのような消費指向を逆手にとり、付加価値の高いブランド品をそっくり真似て製作された偽造品が市場に出回って、安価に大量に販売されることもままある。偽造品の模倣技術が向上し、取り締まりをのがれて流通経路が巧妙に形成され、ブランド品市場において偽造品が本物の製品である真正品のシェアを奪うようになった。メーカにとっては自社の製品の売上が落ちるばかりでなく、偽造品が引き起こすトラブルによる信用の低下でブランドの価値を大きく損なうなど、多大な経済的損失を被る。

【０００４】

また、偽造品を判別できない販売業者や流通業者は、偽造品を真正品と思い込んで取り扱ってしまう。取扱品が偽造品と発覚したときには不良在庫を大量に抱え込むことになり、偽造品を既に販売していた場合には購入者への保証として偽造品の回収や真正品との交換など、多大な経済的損失を被ることになる。

【０００５】

また、偽造品を判別できずに真正品と思い込んで購入した消費者は、購入後にそれが偽造品であるとわかっても、購入地が海外の旅行先などの場合には返品交渉が困難であり、帰国後に故障などのトラブルが生じても販売業者の連絡先がわからない、手続きが面倒などの理由で返品や交換ができないため、やはり経済的損失を被ることになる。

以上に述べたように、偽造品はメーカから販売業者、流通業者を介して消費者に至るまでの、流通経路を形成するものすべてに損害を与える。

【０００６】

そこで、メーカは自社製品と偽造品を判別するために、以下のような対策を講じてきた。

メーカは、自社製品が真正品であることを特徴づける手段として、製品に高度な技巧を凝らす場合がある。具体的には、素材に型押し加工などを施したり、デザインに形状や色彩の複雑なパターンを設けたり、熟練した手作業による細工を施したり、登録商標やロゴマークなどを特定箇所に配置したりする。これはデザインとしての付加価値を高める効果もあるが、模倣を技術的に困難にして偽造を

防ぐ効果もある。

このような場合の真贋判定は、特徴づけた部分において製品が真正品に十分に似ていれば真正品と判定されるし、十分に似ていなければ偽造品と判定される。

【０００７】

また、メーカは、製品を保証するための保証書や保証カードを発行して製品に添付する場合がある。保証書等には固有の製造番号を記載または刻印したり、模倣が技術的に困難な押印や透かしなどの技巧を施したりする。

このような場合の真贋判定は、製品に保証書等が添付されており、その保証書等が真正の保証書等に十分に似ていれば真正品と判定されるし、十分に似ていなければ偽造品と判定される。

【０００８】

さらに、メーカは、模倣が技術的に困難なホログラムなどを施したシールを用いて製品の包装を封印し、容易に開封されない工夫を施す場合がある。

このような場合の真贋判定は、製品の包装を封印したシールを開封した形跡がなければ真正品と判定されるし、開封した形跡があれば偽造品と判定される。

【０００９】

【発明が解決しようとする課題】

これまでに述べた従来の方法によって、ある製品が真正品であるか偽造品であるかを判別して真正品を認証する場合に、以下のような問題がある。

まず、デザインの技巧や登録商標などの表示は、模倣精度を高めれば十分に真正品に似せることができる。よって、判別のためには微妙な違いを見極めるための専門的な知識や技能が必要となり、判別者を養成したり雇い入れたりしなければならない。それでも真正品と模造品の見分けがつかなければ判別はできない。

【００１０】

また、製品に添付する保証書の場合も同様に、模倣精度を高めれば十分に真正の保証書に似せることができる。よって、偽造品に添付された偽造保証書が真正品に添付された真正保証書と見分けがつかなければ、真正品と偽造品の判別ができない。さらに、押印や透かしなどの技巧を施した場合は、違いを見極めるための専門的な知識や技能が新たに必要となり、専門知識や技能が十分でないと、一

見似ている程度の模倣でも安易に信用してしまうなどの逆効果もある。

【００１１】

さらに、包装をホログラムなどの技巧を施したシールで封印した場合は、購入者が購入前に開封できないために内容物を吟味できず、購買意欲の低下を招くというデメリットが生じる。また、シールの製造に余分なコストが掛かる。さらに、上記保証書の場合と同様にホログラムなどの技巧を施した場合は、判別のための専門的な知識や技能が新たに必要となり、専門知識や技能が十分でないと、一見似ている程度の偽造シールでも判別できない。

【００１２】

以上の理由から、製品自体、保証書、封印シールなどの外観上の違いを人為的に判別するという従来の方法は、判別のための専門的な知識や技能を必要とする上に判別作業時間を要する。よって、流通段階において、低コストで容易に任意の場所において短時間で大量に正確に判別することはできない。

【００１３】

本発明は、前記従来における商品流通市場での真性品と偽造品との判別の課題に鑑み、商品の真贋の判別基準を外観上の差異以外に設け、さらに判別方法は人為的な作業ではなく機械的な処理によって効率よく行うようにすることが出来、また商品を取り扱う流通業者や販売点がインターネットを介して簡便に真贋判定を利用出来るようにすることを目的とするものである。

【００１４】

【課題を解決するための手段】

本発明では前記のような目的を達成するため、以下のような製品認証システムを確立するものである。

製品認証システムを構成するハードウェアとして、非接触タグ、リーダ、データベース、データサーバ、認証サーバを用意する。

【００１５】

非接触タグは、認証対象の製品に認証素子として埋め込まれるもので、製品認証システムの管理者しか知り得ない固有のＩＤを持ち、ＩＤを電子データとして本体に記録させる。

リーダは、非接触タグのＩＤデータを読み取るもので、製品認証システムの管理者しか知り得ない固有のＩＤを持ち、ＩＤを電子データとして本体に記録させ、インターネットに接続して通信する手段を持つ。

【００１６】

データベースは、非接触タグのＩＤおよび付帯情報のデータ、非接触タグが埋め込まれた製品情報のデータ、リーダのＩＤおよび付帯情報のデータを格納するもので、インターネットに接続して通信する手段を持つ。

データサーバは、データベースに格納されたデータの読み出しやデータベースへのデータの書き込みを行うもので、インターネットに接続して通信する手段を持つ。

【００１７】

認証サーバは、インターネットに接続されたリーダから送信されたリーダのＩＤデータおよび非接触タグのＩＤデータをデータベースに格納されたデータと照合して、リーダおよび非接触タグの認証を行うもので、インターネットに接続して通信する手段を持つ。

【００１８】

このようなハードウェアを使用し、以下のような手順で製品の真性品であるか否かの認証を行う。

まず、製品認証システムの利用者に非接触タグおよびリーダを配布する前に、データサーバが非接触タグおよびリーダのＩＤデータを読み込み、データファイルを作成してデータベースに格納する。

【００１９】

製品認証システムの利用者に非接触タグおよびリーダが配布された後に、インターネットに接続されたリーダが自分自身のＩＤデータを読み込んで認証サーバに送信し、認証サーバが受信したリーダのＩＤデータをデータベースに格納されたリーダのデータファイルと照合する。

【００２０】

認証サーバが、同一のＩＤデータとの照合がなされたリーダに対してリーダが認証された旨を通知し、製品に埋め込まれた非接触タグのＩＤデータの送信を促

す。

認証されたリーダが、製品に埋め込まれた非接触タグのＩＤデータを読み込んで認証サーバに送信し、認証サーバが受信した非接触タグのＩＤデータをデータベースに格納された非接触タグのデータファイルと照合する。

【００２１】

認証サーバが、同一のＩＤデータとの照合がなされた非接触タグが認証された旨を、非接触タグのＩＤデータを送信したリーダに対して通知する。

また、上記の製品認証システムをアプリケーションサービスプロバイダ（ＡＳＰ）事業者が管理および運営して、インターネットを介した製品認証サービスをＡＳＰ方式で提供することもできる。

【００２２】

また、上記の製品認証システムにおいて、リーダの利用者に対してリーダの管理者および利用者しか知り得ない固有のパスワードを割り当てることにより、利用者側に２重のＩＤを持たせた場合には、以下の手順を加えることにより製品認証システム全体で３重のチェック機能を持たせることができる。

【００２３】

データサーバが、割り当てられたパスワードのデータを配布されたリーダのＩＤデータと対応づけた付帯情報としてデータファイルを作成し、データベースに格納する。

認証サーバが、リーダの認証通知後に利用者のパスワード入力を要求し、利用者の端末から入力され送信されたパスワードのデータを受信し、データベースに格納されたデータファイルと照合する。

認証サーバが、同一のパスワードデータとの照合がなされた場合に、パスワードが認証された旨をパスワードデータを送信した利用者端末に対して通知する。

【００２４】

また、上記の製品認証システムに以下の手順を加えることができる。

製品認証システムの利用者である製品のメーカに配布されたリーダおよび利用者端末が、製品の名称、型式、製造年月日、製造場所などの製品情報データを非接触タグのＩＤデータと対応づけてデータサーバに送信する。

データサーバが製品情報を受信して、埋め込まれた非接触タグのＩＤデータと対応づけた付帯情報としてデータファイルを作成し、データベースに格納する。

【００２５】

上記の手順を加えることにより、例えば安価な真正品に取り付けられた非接触タグの埋め込み部分を取り外して、真正品とは別の高価な製品を模倣した偽造品に取り付け、偽造品の認証を受けて販売しようとする場合に、非接触タグのＩＤ以外に製品名称や型式などの製品情報を参照することにより、上記のような悪用を防ぐことができる。なお、ここで言う「メーカ」とは、製造元以外に、発売元や輸入元等を指す。

【００２６】

さらに、上記の製品認証システムに以下の手順を加えることができる。

非接触タグの製造メーカが、非接触タグのＩＤと非接触タグの供給先である製品のメーカを対応づけたデータファイルを作成して、データサーバに送信する。

データサーバが、データファイルを受信してデータベースに格納する。

認証サーバが、リーダから送信された非接触タグのＩＤデータを受信して、データベースに格納された非接触タグのデータファイルでＩＤと供給先の対応を照合する。

【００２７】

以上の手順によって、製品の認証が２段階になる。つまり、はじめに非接触タグのＩＤと供給先との対応を確認し、後に非接触タグのＩＤと製品情報との対応を確認することになるため、偽造品の検出をより効率的に行うことができると同時に、より信頼度を高めることができる。

【００２８】

【発明の実施の形態】

次に、図面を参照しながら、本発明の実施の形態について、具体的且つ詳細に説明する。

まず、本発明による製品認証システムの一実施態様について、その概要を図１を参照しながら説明する。

【００２９】

製品認証システムの当事者は、管理者であるＡＳＰ事業者１０、利用者であるメーカ２０、販売業者３０、流通業者４０、消費者５０である。ＡＳＰ事業者１０は、非接触タグ１１およびリーダ１２を管理して製品認証システムを管理・運営し、製品認証サービスを提供する。

【００３０】

ＡＳＰ事業者１０は、メーカ２０に対して非接触タグ１１を供給する。非接触タグ１１は固有のＩＤを持ち、ＩＤが電子データとして本体に記録されているものである。ＡＳＰ事業者１０は、非接触タグ１１のＩＤデータおよび供給先であるメーカ名などの付帯情報のデータを管理する。

【００３１】

上記の非接触タグ１１の供給については、非接触タグ１１の製造メーカが、メーカ２０に直接非接触タグ１１を供給することもできる。この場合は、非接触タグ１１の製造メーカが、非接触タグ１１のＩＤと供給先である商品のメーカ２０を対応づけたデータファイルを作成して、ＡＳＰ事業者１０にデータを提供することもできる。

【００３２】

非接触タグ１１としては、通信機能付き超小型ＩＣチップを使用することが出来る。このような通信機能付き超小型ＩＣチップとしては、例えば日立製作所製の商品名ミューチップ（μチップ）を挙げることが出来る。このチップは、縦と横がそれぞれ〇・四mm、厚さは約一七〇μmと指先に載せてもほんの点にしか見えない。その中に一二八ビットのメモリーと二・四五ギガヘルツの電波で通信できる機能を有する。

【００３３】

ＡＳＰ事業者１０は、製品認証サービスの各利用者に対して前記非接触タグ１１のＩＣコードを読み取るリーダ１２を貸与する。リーダ１２は、パソコンなどの汎用の端末装置を介してインターネットに接続することができ、固有のＩＤを持ち、ＩＤが電子データとして本体に記録されているものである。ＡＳＰ事業者１０は、リーダ１２のＩＤデータおよび貸与先である利用者名などの付帯情報のデータを管理する。

【００３４】

ＡＳＰ事業者１０は、リーダ１２の貸与に際し、利用者に対して固有のパスワードを割り当てることにより、利用者側に２重のＩＤを持たせることもできる。ＡＳＰ事業者１０は、割り当てたパスワードのデータをリーダ１２の付帯情報のデータとして管理する。

【００３５】

メーカ２０は、ＡＳＰ事業者１０から供給された非接触タグ１１を製品に埋め込む。外観上はわからないように製品の内部に埋め込むことで、製品の美観を損ねることがなく、取り外して悪用されるのを防止できる。メーカ２０は、貸与されたリーダ１２をインターネットに接続する。メーカ２０は、リーダ１２の認証を受けた上で、非接触タグ１１に対応する製品の名称、製造年月日、製造場所などの製品情報をＡＳＰ事業者１０に登録する。ＡＳＰ事業者１０は、非接触タグ１１のＩＤ、供給先であるメーカ名に加えて、メーカ２０から登録された製品情報のデータを対応づけて管理する。

メーカ２０は、リーダ１２の認証を受けた上で、登録したデータを閲覧することができる。

【００３６】

販売業者３０および流通業者４０は、貸与されたリーダ１２をインターネットに接続する。販売業者３０および流通業者４０は、リーダ１２の認証を受けた上で、取り扱う製品が真正品であることの認証をＡＳＰ事業者１０に照会する。ＡＳＰ事業者１０は、照会された非接触タグ１１のＩＤデータと管理するデータとを照合して製品の認証を行い、販売業者３０および流通業者４０に通知する。

【００３７】

消費者５０は製品の購入時に、販売業者３０に対して、販売業者３０がその製品に対して認証を取得したという証拠の提示を要求することができる。販売業者３０は消費者５０に対して、その製品の認証を取得したという証拠を提示する。消費者５０は、新品の購入時に限らず中古品の売買時においても、任意の販売業者３０に対して製品認証を要求し、製品認証を取得した証拠の提示を要求することができる。

【００３８】

次に、本発明による製品認証システムの前記実施態様を実現するハードウェアの構成について、図２を参照しながら説明する。

製品認証サービスの提供者であるＡＳＰ事業者１０は、インターネット上でデータの受け渡しをするためのデータベース１３、データサーバ１４、認証サーバ１５を管理する。

【００３９】

製品認証サービスの利用者であるメーカ２０、販売業者３０、流通業者４０は、ＡＳＰ事業者１０から貸与されたリーダ１２を保持し、リーダ１２をインターネットに接続するためのパソコンなどの汎用端末装置２１、３１、４１を持つ。

ＡＳＰ事業者１０は、メーカ２０に非接触タグ１１を供給する。メーカ２０は、非接触タグ１１を埋め込んだ製品を、販売業者３０あるいは流通業者４０に出荷する。

販売業者３０および流通業者４０は、流通段階で製品を取扱い、販売業者３０は最終的に消費者５０に製品を販売する。

【００４０】

次に、本発明による製品認証システムの前記実施態様を実現するため、前記ハードウェアにより行われる情報の処理について、図３を参照しながら詳細に説明する。

まず、メーカ２０による製品情報の登録、閲覧は以下の手順で行われる。

メーカ２０は、非接触タグ１１を埋め込んで製造した製品の名称、製造年月日、製造場所などの製品情報をもとにデータファイルを作成する。メーカ２０は、端末装置２１を介してリーダ１２をインターネットに接続する。リーダ１２は、自分自身のＩＤデータを認証サーバ１５に送信する。認証サーバ１５は、受信したリーダ１２のＩＤデータを、データベース１３に格納されたリーダ１２のデータファイルと照合する。照合されれば認証サーバ１５は自動的にメーカ２０の端末装置２１にリーダ１２の認証を通知する。

【００４１】

さらに、パスワードが割り当てられている場合は、認証サーバ１５がパスワー

ドを要求し、入力されたパスワードデータをデータベース１３のデータファイルと照合して、照合されれば利用者の認証を通知する。

それからメーカ２０は、データサーバ１４に対して製品情報の登録を要求し、非接触タグ１１のＩＤと対応させながら製品情報データファイルを送信する。データサーバ１４は、受信した製品情報データファイルを予め登録してあった非接触タグ１１のデータファイルと対応づけて非接触タグ１１のデータファイルを更新し、データベース１３に格納する。

【００４２】

メーカ２０は、リーダ１２の認証、パスワードの認証を受けた上でデータサーバ１４に対して製品情報の閲覧を要求する。データサーバ１４はデータベース１３から非接触タグ１１のデータファイルを読み出して、製品情報データをメーカ端末２１に送信する。メーカ２０はメーカ端末２１上で製品情報を閲覧する。

【００４３】

次に、販売業者３０および流通業者４０による製品の認証取得は以下の手順で行われる。

まず販売業者３０および流通業者４０は端末装置３１、４１を介してリーダ１２をインターネットに接続する。リーダ１２は、自分自身のＩＤデータを認証サーバ１５に送信する。認証サーバ１５は、受信したリーダ１２のＩＤデータを、データベース１３に格納されたリーダ１２のデータファイルと照合する。照合されれば認証サーバ１５は自動的に販売業者３０および流通業者４０の端末装置３１、４１にリーダ１２の認証を通知する。

【００４４】

さらに、パスワードが割り当てられている場合は、認証サーバ１５がパスワードを要求し、入力されたパスワードデータをデータベース１３のデータファイルと照合して、照合されれば利用者の認証を通知する。

それから販売業者３０および流通業者４０は、受け取った製品が真正品であることを確認するために、リーダ１２で製品に埋め込まれた非接触タグ１１のＩＤを読み取る。すると認証サーバ１５は自動的に非接触タグ１１のＩＤを読み取り、データベース１３に格納された非接触タグ１１のデータファイルと照合する。

このとき、認証サーバ１５は非接触タグ１１のＩＤと供給先であるメーカ２０との対応を確認することによって、偽造品の判別を行うこともできる。照合されれば認証サーバ１５は、自動的に販売業者３０および流通業者４０の端末装置３１、４１に非接触タグ１１の認証を通知するとともに、付帯情報として管理されている製品の型式など製品情報の一部を開示する。販売業者３０および流通業者４０は、開示された製品の型式などの製品情報と認証された製品を比較して、製品が真正品であることを確認する。

【００４５】

仮に、製品認証システムを不正に利用しようとした場合について、図４を参照しながら説明する。

まず、正規に利用する場合について説明すると、ＡＳＰ事業者１０と契約して製品認証サービスを受ける正規の販売業者３０は、ＡＳＰ事業者１０から貸与されたリーダ１２が持つ固有のＩＤにより、自動的にリーダ１２の認証を受けることができる。さらに、この販売業者３０にＡＳＰ事業者１０からパスワードが割り当てられている場合は、パスワードの照合によって利用者の認証を受けることができる。販売業者３０は真正品に埋め込まれた非接触タグ１１のＩＤをリーダ１１で読み取ることによって、自動的に製品の認証を受けることができる。製品が偽造品であれば、非接触タグ１１が埋め込まれていないために製品の認証は受けられず、自動的に偽造品を判別することができる。

【００４６】

次に、不正利用者がＡＳＰ事業者１０から正規の利用者に貸与されたリーダ１２を盗んで製品認証システムを不正に利用しようとした場合について説明する。不正業者は自動的にリーダ１２の認証を受けることができるが、ＡＳＰ事業者１０からパスワードを要求された場合には、正規利用者に割り当てられたパスワードを知らないので正しいパスワードを入力できないため、利用者の認証を受けることができない。よって、不正利用者は製品認証サービスを受けられない。

【００４７】

さらに、不正利用者がリーダを偽造して製品認証システムを不正に利用しようとした場合について説明すると、不正利用者は偽造リーダをインターネットに接

続しても、ＡＳＰ事業者１０からリーダの認証を受けることができない。よって、不正利用者は製品認証サービスを受けられない。

【００４８】

【発明の効果】

以上説明した通り、本発明では、製品の真贋判別基準を従来の外観以外に設けること、真贋判別作業を従来の人為的な目視判断に依らず機械的な電子情報処理作業に依ることを課題とし、それらを解決した製品認証システムをインターネット上に構築し、製品の流通経路を形成するメーカ、販売業者、流通業者に対して、インターネット上の製品認証サービスとしてＡＳＰ方式で提供することにより、メーカの工場出荷から小売店の店頭入荷に至るまでの製品の流通段階ごとに、低コストで容易に任意の場所において短時間で大量に正確に、真正品と偽造品の判別が実現できる。

【００４９】

また、上記の製品認証システムにおいて、リーダに固有のＩＤを持たせ、さらに利用者に固有のパスワードを割り当てて管理することにより、リーダの盗難や偽造による製品認証システムの不正利用を防止することができる。

したがって、市場に出回る偽造品が流通経路に侵入するのを防ぎ、製品を製造するメーカをはじめとして、製品を取り扱う販売業者および流通業者、製品を購入する消費者に至るまで、製品に関わり流通経路を形成するすべての製品認証システム利用者の利益を保護することができる。

【図面の簡単な説明】

【図１】

本発明による製品認証システムの一実施形態の概要を説明した図で、ものおよび情報の流れを示すことによりシステムの当事者の役割を説明する。

【図２】

前記製品認証システムの実施形態を実現するために必要なハードウェアの構成を説明した図で、当事者ごとに具備すべきハードウェアを示す。

【図３】

前記図２に示したハードウェアにより製品認証システムの実施形態を実現する

ための情報処理について詳細に説明した図で、ハードウェア間でやりとりされる情報の内容および方向を示す。

【図４】

前記製品認証システムを不正に利用しようとした場合の製品認証システムの応答について、正常に利用した場合と比較して説明した図である。

【符号の説明】

１０　ＡＳＰ

１１　非接触タグ

１２　リーダ

１３　データベース

１４　データサーバ

１５　認証サーバ

２０　メーカ

２１　メーカのインターネット接続のための汎用端末装置

３０　販売業者

３１　販売業者のインターネット接続のための汎用端末装置

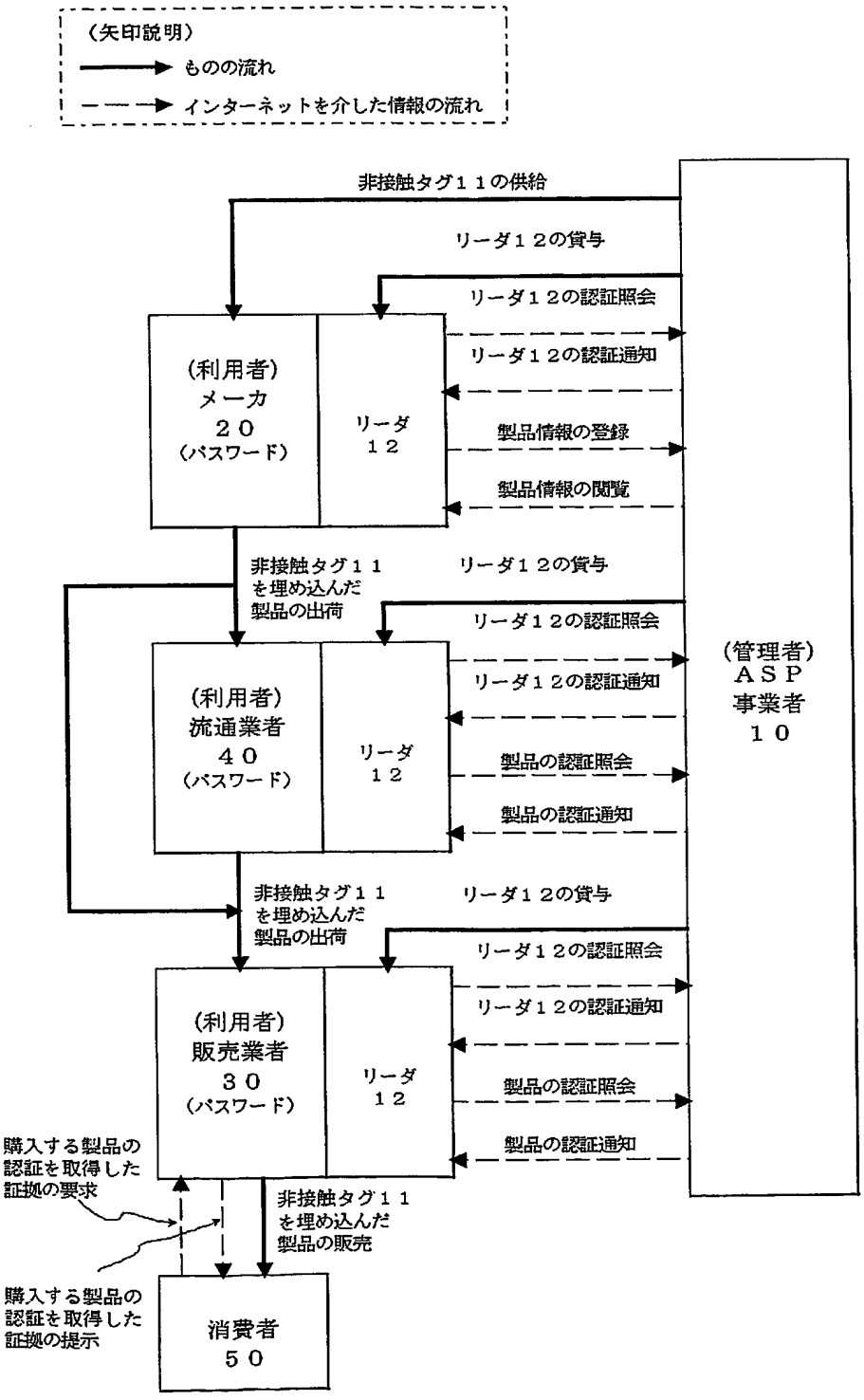
４０　流通業者

４１　流通業者のインターネット接続のための汎用端末装置

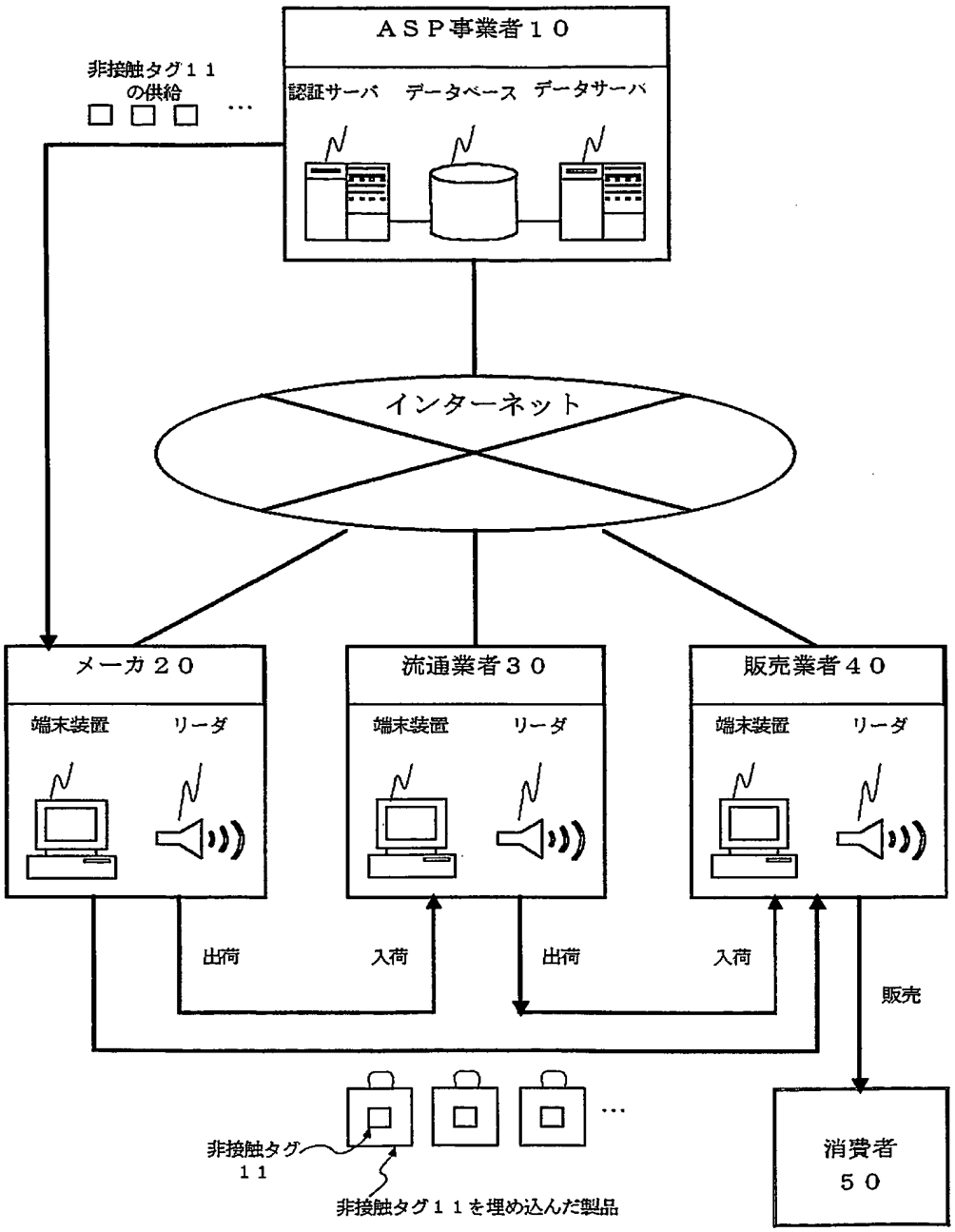
５０　消費者

【書類名】　　図　面

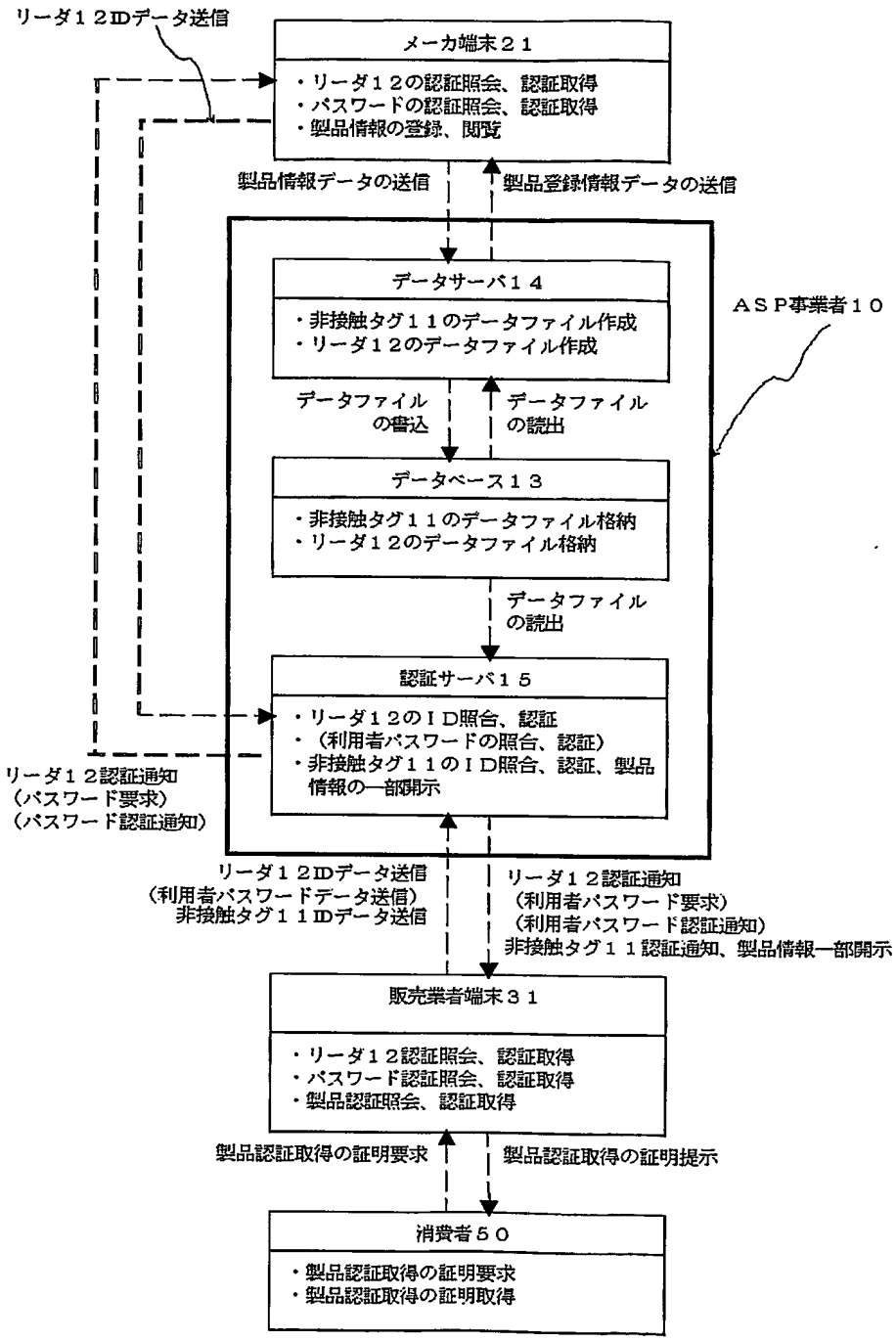
【図１】


（矢印説明）
ものの流れ
インターネットを介した情報の流れ
非接触タグ１１の供給
リーダ１２の貸与
リーダ１２の認証照会
リーダ１２の認証通知
製品情報の登録
製品情報の閲覧
（利用者）
メーカ
２０
（パスワード）
リーダ
１２
非接触タグ１１
を埋め込んだ
製品の出荷
リーダ１２の貸与
リーダ１２の認証照会
リーダ１２の認証通知
製品の認証照会
製品の認証通知
（利用者）
流通業者
４０
（パスワード）
リーダ
１２
非接触タグ１１
を埋め込んだ
製品の出荷
リーダ１２の貸与
リーダ１２の認証照会
リーダ１２の認証通知
製品の認証照会
製品の認証通知
（利用者）
販売業者
３０
（パスワード）
リーダ
１２
（管理者）
ＡＳＰ
事業者
１０
購入する製品の
認証を取得した
証拠の要求
非接触タグ１１
を埋め込んだ
製品の販売
購入する製品の
認証を取得した
証拠の提示
消費者
５０

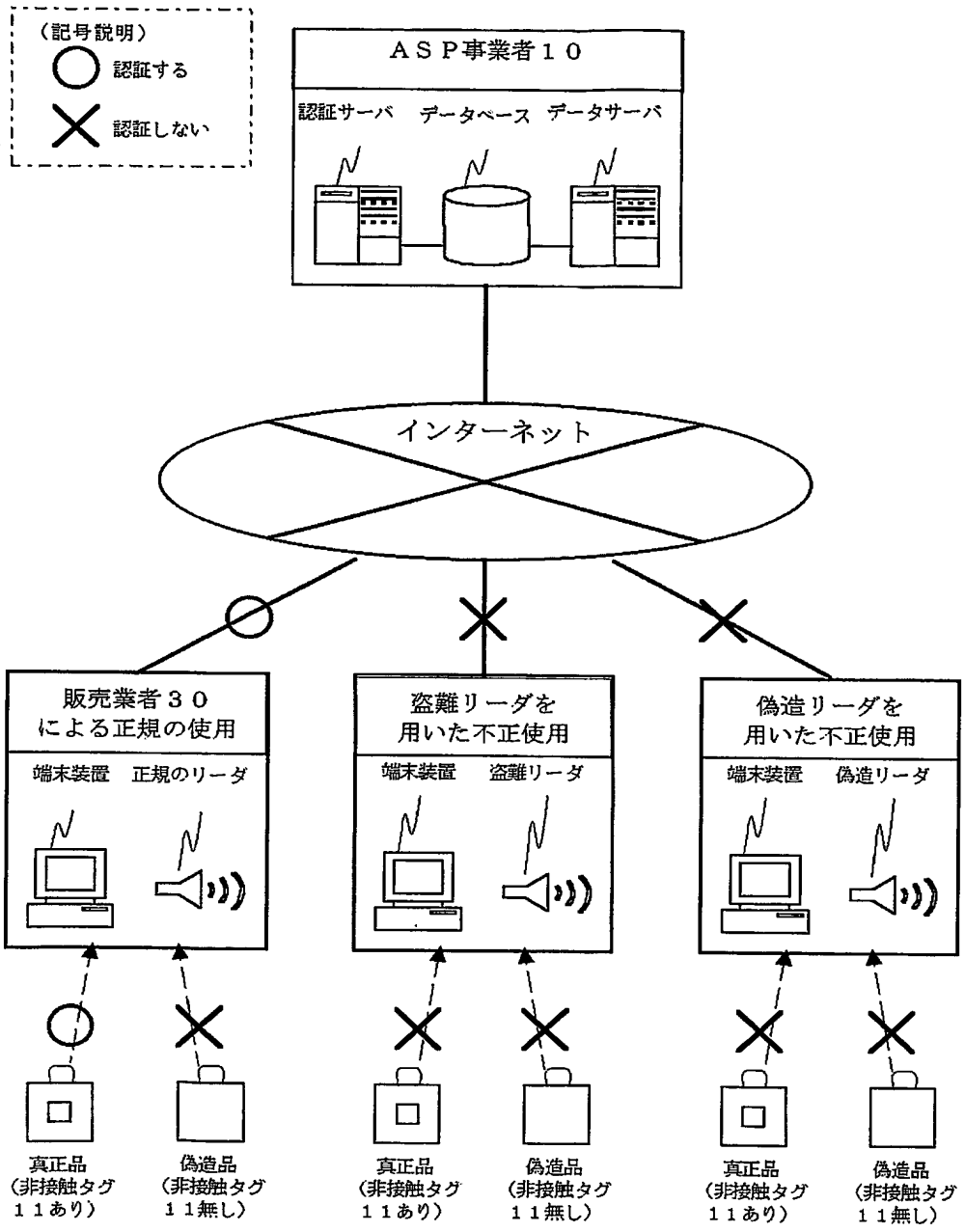
【図２】


ＡＳＰ事業者１０
認証サーバ
データベース
データサーバ
非接触タグ１１
の供給
インターネット
メーカ２０
端末装置
リーダ
流通業者３０
端末装置
リーダ
販売業者４０
端末装置
リーダ
出荷
入荷
出荷
入荷
販売
非接触タグ
１１
非接触タグ１１を埋め込んだ製品
消費者
５０

【図３】


リーダ１２IDデータ送信
メーカ端末２１
・リーダ１２の認証照会、認証取得
・パスワードの認証照会、認証取得
・製品情報の登録、閲覧
製品情報データの送信
製品登録情報データの送信
ASP事業者１０
データサーバ１４
・非接触タグ１１のデータファイル作成
・リーダ１２のデータファイル作成
データファイル
の書込
データファイル
の読出
データベース１３
・非接触タグ１１のデータファイル格納
・リーダ１２のデータファイル格納
データファイル
の読出
認証サーバ１５
・リーダ１２のＩＤ照合、認証
・（利用者パスワードの照合、認証）
・非接触タグ１１のＩＤ照合、認証、製品情報の一部開示
リーダ１２認証通知
（パスワード要求）
（パスワード認証通知）
リーダ１２IDデータ送信
（利用者パスワードデータ送信）
非接触タグ１１IDデータ送信
リーダ１２認証通知
（利用者パスワード要求）
（利用者パスワード認証通知）
非接触タグ１１認証通知、製品情報一部開示
販売業者端末３１
・リーダ１２認証照会、認証取得
・パスワード認証照会、認証取得
・製品認証照会、認証取得
製品認証取得の証明要求
製品認証取得の証明提示
消費者５０
・製品認証取得の証明要求
・製品認証取得の証明取得

【図４】


（記号説明）
認証する
認証しない
ＡＳＰ事業者１０
認証サーバ　データベース　データサーバ
インターネット
販売業者３０
による正規の使用
端末装置　正規のリーダ
盗難リーダを
用いた不正使用
端末装置　盗難リーダ
偽造リーダを
用いた不正使用
端末装置　偽造リーダ
真正品
（非接触タグ
１１あり）
偽造品
（非接触タグ
１１無し）
真正品
（非接触タグ
１１あり）
偽造品
（非接触タグ
１１無し）
真正品
（非接触タグ
１１あり）
偽造品
（非接触タグ
１１無し）

【書類名】　　要約書

【要約】

【課題】　市場に出回る偽造品が流通経路に侵入するのを防ぐ。

【解決手段】　データサーバが非接触タグ１１およびリーダ１２のＩＤデータを読み込み、データファイルを作成してデータベースに格納する。インターネットに接続されたリーダ１２が自分自身のＩＤデータを読み込んで認証サーバに送信し、認証サーバが受信したリーダ１２のＩＤデータをデータベースに格納されたリーダ１２のデータファイルと照合し、一致すればリーダ１２を認証する。認証されたリーダ１２が、製品に埋め込まれた非接触タグ１１のＩＤデータを読み込んで認証サーバに送信し、認証サーバが受信した非接触タグ１１のＩＤデータをデータベースに格納された非接触タグのデータファイルと照合し、その結果一致すれば認証された旨をリーダ１２に通知する。この製品認証システムは、アプリケーションサービスプロバイダ（ＡＳＰ）事業者１０が管理および運営する。

【選択図】　　図２

職権訂正履歴（職権訂正）

特許出願の番号	特願２００３－０４０６９２
受付番号	５０３００２６１２８５
書類名	特許願
担当官	末武　実　　１９１２
作成日	平成１５年　２月２１日

＜訂正内容１＞
訂正ドキュメント
書誌
訂正原因
職権による訂正
訂正メモ
【特許出願人】の欄の記載に誤りがあり訂正します。
訂正前内容
【特許出願人】
　【住所又は居所】　３９１０５１３６０
　【氏名又は名称】　千代田メインテナンス株式会社
訂正後内容
【特許出願人】
　【識別番号】　３９１０５１３６０
　【氏名又は名称】　千代田メインテナンス株式会社

次頁無

認定・付加情報

特許出願の番号	特願２００３－０４０６９２
受付番号	５０３００２６１２８５
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　３月　４日

＜認定情報・付加情報＞

【提出日】	平成15年 2月19日
【特許出願人】	
【識別番号】	391051360
【住所又は居所】	茨城県鹿島郡旭村箕輪１６３２番地
【氏名又は名称】	千代田メインテナンス株式会社
【代理人】	申請人
【識別番号】	100081927
【住所又は居所】	茨城県水戸市千波町２４３２番地の３７
【氏名又は名称】	北條　和由

次頁無

特願２００３－０４０６９２

出　願　人　履　歴　情　報

識別番号　　[３９１０５１３６０]

１．変更年月日　　１９９７年　２月２８日
[変更理由]　　住所変更
住　所　　茨城県鹿島郡旭村箕輪１６３２番地
氏　名　　千代田メインテナンス株式会社